

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-256746

(43)Date of publication of application : 12.09.2003

(51)Int.Cl.

G06F 17/60  
B42D 15/10  
G06K 17/00  
G06K 19/00  
G06K 19/10  
G06T 1/00  
G06T 7/00  
G07F 7/12  
H04L 9/32

(21)Application number : 2002-052670

(71)Applicant : OMRON CORP

(22)Date of filing : 28.02.2002

(72)Inventor : KOJI RYOICHI

## (54) TRANSACTION PROCESSING DEVICE, TRANSACTION PROCESSING SYSTEM, AND TRANSACTION PROCESSING METHOD

### (57)Abstract:

PROBLEM TO BE SOLVED: To prevent an illegal use of a credit card more effectively than in a conventional method.

SOLUTION: A CAT (credit authorization terminal) 1 is provided with a card reader part 9 reading face image data from the card, a face feature point extraction part 14 for extracting feature points from the face image data read by the card reader part 9 as feature point data, a communication circuit 13 for sending the feature point data extracted by the face feature point extraction part 14 to a host computer 3, and a display part 10 for displaying the face image data read by the card reader part 9 and results of certification sent from the host computer 3.



### LEGAL STATUS

[Date of request for examination]

15.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-256746

(P2003-256746A)

(43) 公開日 平成15年9月12日 (2003.9.12)

(51) Int.Cl.	識別記号	F I	テ-マ-ド (参考)	
G 0 6 F 17/60	4 1 4	G 0 6 F 17/60	4 1 4	2 C 0 0 5
	4 0 2		4 0 2	3 E 0 4 4
	5 1 0		5 1 0	5 B 0 3 5
B 4 2 D 15/10	5 0 1	B 4 2 D 15/10	5 0 1 B	5 B 0 5 7
	5 2 1		5 2 1	5 B 0 5 8
審査請求 未請求 請求項の数 4 O L (全 11 頁) 最終頁に続く				

(21) 出願番号 特願2002-52670 (P2002-52670)

(22) 出願日 平成14年2月28日 (2002.2.28)

(71) 出願人 000002945

オムロン株式会社

京都市下京区塩小路通堀川東入南不動堂町  
801番地

(72) 発明者 興治 良一

京都府京都市下京区塩小路通堀川東入南不  
動堂町801番地 オムロン株式会社内

(74) 代理人 100085008

弁理士 世良 和信 (外1名)

最終頁に続く

(54) 【発明の名称】 取引処理装置、取引処理システムおよび取引処理方法

(57) 【要約】

【課題】 クレジットカードの不正使用をより効果的に防止すること。

【解決手段】 カードから顔画像データを読み取るカードリーダー部9と、カードリーダー部9により読み取られた顔画像データから特徴点を特徴点データとして抽出する顔面特徴点抽出部14と、顔面特徴点抽出部14により抽出された特徴点データをホストコンピュータ3に送信する通信回路13と、カードリーダー部9により読み取られた顔画像データの表示、およびホストコンピュータ3から送信された認証結果を表示する表示部10と、を備えたC A T 1。



## 【特許請求の範囲】

【請求項1】カードから顔画像データを読み取る読取手段と、

前記読取手段により読み取られた顔画像データから特徴点を特徴点データとして抽出する特徴点抽出手段と、前記特徴点抽出手段により抽出された特徴点データをセンタ装置に送信する送信手段と、

前記読取手段により読み取られた顔画像データの表示、および前記センタ装置から送信された認証結果を表示する表示手段とを備えた取引処理装置。

【請求項2】カードから顔画像データを読み取る読取手段と、

前記読取手段により読み取られた顔画像データから特徴点を特徴点データとして抽出する特徴点抽出手段と、前記特徴点抽出手段により抽出された特徴点データを送信する送信手段と、

前記読取手段により読み取られた顔画像データの表示、および前記特徴点データに基づいた認証結果を表示する表示手段と、を備えた取引処理装置と、前記取引処理装置から前記特徴点データが送信され、送信された前記特徴点データに基づいて認証を行う認証手段を備えたセンタ装置と、からなる取引処理システム。

【請求項3】前記カードの利用が正規ユーザによる利用かどうかの判定を一定の閾値を基準にして判定する請求項2記載の取引処理システム。

【請求項4】カードから顔画像データを読み取り、

顔画像データから特徴点を抽出し、

抽出された特徴点をセンタ装置に送信し、

顔画像データに基づいて顔画像およびセンタ装置から送信された認証結果を表示する取引処理方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明はクレジットカードの不正使用を防止する取引処理技術に関する。

## 【0002】

【従来の技術】クレジットカード（以下特に断らない限り「カード」という。）は現金を持ち歩かなくても買物ができるという利便性から普及し、今日、キャッシュレス社会を実現するまでにいたっている。

【0003】しかしながらクレジットカードを利用した不正が後を絶たない。このため、クレジットカード会社は、加盟店にクレジットカード認証端末であって取引処理装置として機能するCAT（クレジット・オーソライゼーション・ターミナル）を設置してもらい、顧客が提示したカードが不正使用されていないか否かをその場で判定する防犯システムを採用している。

## 【0004】

【発明が解決しようとする課題】カードを紛失したり盗難にあたりした場合、最寄りの警察やカード会社に連

絡し、自己所有のカードの利用を差し止めて他人による不正使用を防止するようになっているけれども、紛失や盗難にあったことをすぐには気付かない場合がある。

【0005】その場合、被害届けが出される前に第三者による不正使用がなされると、CATを用いた防犯システムを採用していても回避できない場合が少なくない。

【0006】周知のごとくカードを利用するにあたり、利用者は伝票にサインし、加盟店側ではカードに記載された正規ユーザによる自署と一致するか否かをチェックするようにはなっている。しかしながら、確信がない以上、不正の有無を客側に問い質すことは、正規ユーザによるカード利用であったことを考慮すると店のイメージダウンにも繋がるため多くはない。

【0007】また、正規ユーザの顔の特徴点をカードに記憶させておき、カード利用者の不正をチェックするシステムが採用されているが、利用者の顔から特徴点を認識するには、その利用者の顔を店員が注視する必要があり、やはり店のイメージダウンにつながる。

【0008】このため不審なカード利用者とは思ってもカードの利用を許諾してしまう加盟店も少なくなく、よってカード会社が損害を補償するケースが後を絶たない。

【0009】クレジットカード会社では、カード表面に本人の写真を貼りつけるなどして防犯に努めているが、写真が張り替えられてしまう虞がある。

【0010】そこで、顔写真データをクレジットカード会社のホストコンピュータに送信して照合するシステムが知られているが、通信中に顔写真データが盗まれてしまうと偽造される虞がある。

【0011】本発明は、上記実情に鑑みてなされたものであり、その解決しようとする課題は、カードの不正使用を従来よりも効果的に防止できる技術を提供することにある。

## 【0012】

【課題を解決するための手段】本発明は、前述の技術的課題を解決するために以下のようにした。

【0013】すなわち、本発明は、カードの内部メモリに正規ユーザの顔面特徴点データを記録しておく。またクレジットカード会社のホストコンピュータには正規ユーザ判定用に顔面特徴点データをデータベース化しておく。

【0014】また当該カードを利用するとCAT上のディスプレイに正規ユーザの顔が表示されるようになっている。よって、正規ユーザによるものか不正な使用者によるものか確認できる。

【0015】さらにCATでカードを読み取ると、正規ユーザの顔面特徴点データが抽出される。また、クレジットカード会社のホストコンピュータにはクレジット利用データが送信される。

【0016】送信された情報が、ホストコンピュータに

記録されている正規ユーザの顔面特徴点データと一致した場合、ホストコンピュータはカード利用者を正規ユーザと特定し、当該カードは正当に利用されているというメッセージをCATの表示部に出す。

【0017】なお、CAT自体にまたはその近傍の店内適所に例えば電子スチルカメラを装備しておき、利用者を撮影する。そして、その生の顔写真データをホストコンピュータに送信し、ホストコンピュータで受信したカード利用者の顔から特徴点を抽出する。この抽出された特徴点を、現在、カードを利用している者の顔面特徴点データとし、当該データをホストコンピュータに記録されている正規ユーザの顔面特徴点データと照合するようにしてもよい。

【0018】よって不正使用の防止を強化できる。

【0019】さらにセキュリティを高められるように前記抽出した顔面特徴点データにスクランブルをかけることもできる。

【0020】顔面照合の代わりに、指紋照合やアイリス照合等に置き換えてもよい。

【0021】ホストコンピュータの真偽判定運用に関しては、一定の閾値を設定し、照合による一致程度が0~60%の場合は無条件にカードの利用を拒絶するようにし、61~80%の場合は不審客として通信手段等の他の確認手段を用いた判定を行ってからカードの利用の可否を行うようにし、81~100%の場合は正規ユーザによる正規なカードの利用が為されているという判定を行うようにすることも考えられる。閾値はパラメータとして運用に応じて変更すると好適である。なお、ホストコンピュータとの間での通信途中に万一特徴点データが盗まれたとしても特徴点だけで正規利用者の顔を復元することは不可能である。よってセキュリティの向上を期待できる。

【0022】

【発明の実施の形態】以下、本発明の実施の形態（以下「実施形態」という）を図示例と共に説明する。

【0023】図1に本発明に係るクレジットカードを利用した商品購入のシステム構成の概略図を示す。

【0024】符号1、2および3は、それぞれCAT、クレジットカードおよびクレジットカード会社の本部（センタ）に設置されたホストコンピュータ（センタ装置）を示す。

【0025】CAT1とクレジットカード会社のホストコンピュータ3とは、公衆回線や専用回線を通じて繋がっている。そして、クレジットカード（以下「カード」という。）2をCAT1で読み込むとカード2に記憶されている各種情報がホストコンピュータ3に電送される。

【0026】次に図2および図3を用いてカード2の構成を示す。

【0027】図2にはカード2の表面に刻まれた各種カ

ード情報（カード表面情報）を示す。カード情報として、例えば正規ユーザ（所有者）のID番号、カード所有者の氏名、カードの有効期限、所有者の顔写真等がカード表面に記載される。これらの情報のうち例えばID番号、本人の氏名、カードの有効期限等は、オフライン運用を図るためにエンボス化してある。

【0028】また、図3はカード2の内部メモリに記憶されている情報の例示である。当該メモリ記憶情報としては例えばカード所有者のID番号、カード所有者の氏名、カードの有効期限、カード所有者の顔画像データ

（当該顔画像データがあればカード所有者の顔をCAT1やホストコンピュータのディスプレイに正確に表示することができる。顔画像データには正規カード所有者の顔の特徴部分についての情報が少なくとも含まれる。なお当該特徴部分の情報を顔面特徴点データということにする。）をデータ化し記憶してある。顔画像データは、デジタル画像として処理される。なおクレジットカードはICカードその他のメモリー媒体方式のカードでも適用できる。

【0029】顔画像データは、カード発行時にカード所有者本人の顔を撮影し、かつこれをデータ化したものである。よって、顔画像データのことを写真データという場合がある。またホストコンピュータ3にも顔画像データや顔面特徴点データが格納される。

【0030】次に図4および図5を参照して、クレジットカード2とCAT1とホストコンピュータ3との関係を説明する。

【0031】なお、図4に示す(I)~(II)の符号および図5に示す(I)~(II)の符号は、同一の符号同士で対応しており、処理の移行先を案内する。例えば、図4の(I)は、図5の(I)と対応しており、図4の(I)に係るルートにおける処理は、図5の(I)に係るルートに移行してそのまま図5で続行されることを意味する。図面についてのこのような対応関係は図6と図7、および図8と図9においても適用される。

【0032】CAT1は、クレジットカード2が有する各種情報を読み取る読取手段としてのカードリーダ部9と、カード表面の顔面写真を表示したり、CAT6のオペレータに種々の指示をしたり各種情報を表示したりする表示手段としての表示部10と、買物金額等を入力するためのテンキー部11と、カードで購入した商品の支払方法について一括払いか分割払か（クレジット金額支払処理区分）の選択をするファンクションキー部12と、カード2から読み取った利用者のID情報や顔面特徴点データをホストコンピュータ3に送受信するための送・受信手段としての通信回路13と、カードリーダ部9によりカード2から情報として読み取った顔面写真からバイオメトリックス技術によって正規ユーザの顔面の特徴点を抽出するための顔面特徴点抽出手段としての顔面特徴点抽出部14と、データを暗号化するための暗号

化回路15と、CAT3を構成する各部に直流電圧を供給する電源回路16と、プリンタ制御部21と、プリンタ制御部21の制御によりクレジット伝票を印刷したり、一日のクレジット売上げ集計を印字したりするプリンタ部22と、CAT全体を制御する制御部24を有する。

【0033】カード会社のホストコンピュータ3は、各店舗に設置してあるCAT1から送信されてくる暗号化された各種データを受け取り、各加盟店に設置してあるCAT1との間でクレジット承認ジョブを実施する通信部17と、通信部17で受け取った暗号化データを解読してもとの値に戻す(解凍する)暗号解読部18と、正規ユーザの前記各種データを予め登録してあるデータベースファイル部19と、データベースファイル部19内の該当者のデータおよび前記暗号解読部18によって解読したデータとを比較判定する判定指示部20と、カード2の利用が正規ユーザによる利用か不正使用者による利用であるかの照合を行うために用いられる閾値を設定する閾値設定部23と、ホストコンピュータ全体を制御する中央演算処理装置であるCPU部25を有する。

【0034】ホストコンピュータ3の暗号解読部18は、前もって収蔵してあるクレジットカード会員のデータからID番号を枕として顔面特徴点データを引き出し、以前同一カードを利用して商品の購入を行った際になされたCAT1から得た先の通信に基づくデータとの突き合わせを行う。

【0035】顔面の特徴点照合判定を行うに際し、閾値設定部23ではバイオメトリックス技術判定を行う。その関係で100%完全な一致をみるには無理がある。よって、閾値のレベルに応じて真偽判定を決める。例えば照合による一致程度が0~60%の場合は無条件にカードの利用を拒絶し、61~80%の場合は不審客として電話その他の通信手段を用いた判定を併用し、その結果をまとめてカード利用の可否を行い、81~100%の場合は正規ユーザによる正規なカード利用が為されているという判定を行う。

【0036】なお、図中の実線矢印は、クレジットカード2、CAT1およびホストコンピュータ3相互において、各種情報や命令の送受信を行うことを目的として、CAT1およびホストコンピュータ3それぞれの構成部同士を連結する配線(バス)やCAT1およびホストコンピュータ3を結ぶ通信経路を示す。また、破線矢印は、クレジットカード2に含まれている正規データが、CAT1のデータベースファイル部19にも記憶され相互にリンクしていることを意味する。

【0037】本システムにあっては、矢印100は、カード利用者がCATのオペレータに差し出すことを示唆する。差し出されたカード2は、CAT1のカードリーダー部9で読み込まれてCAT内部に取り込まれる。

【0038】また、矢印104は、CAT1およびホス

トコンピュータ3を結ぶ前記通信経路であり、CAT1とホストコンピュータ3とが、それぞれの通信手段(CAT1の場合は通信回路13であり、ホストコンピュータ3の場合は通信部17である。)により、公衆回線や専用回線を通じて繋がっていることを示す。

【0039】カードリーダー部9で読み取られたクレジットカード2に含まれている、ID番号、カード所有者の氏名、カードの有効期限、カード所有者の顔写真、当該所有者の顔画像データのデータ、テンキー入力部11で入力された買物金額等のデータ、クレジット金額支払処理区分等ファンクションキー部12で選択されたデータは、制御部24に送られる(矢印106, 108, 110参照)。

【0040】制御部24に送られた情報のうち所有者の顔画像データである写真データは、顔面特徴点抽出部14を経由して(矢印112参照)暗号化回路15に送られる(矢印114参照)。

【0041】暗号化回路15で暗号化されたデータやテンキー部11およびファンクションキー部12による入力データは、通信回路13を経由して通信回路13に送られ(矢印116, 117参照)、その後ホストコンピュータ3の通信部17に送信される(矢印104参照)。

【0042】暗号化するためのキーは、ホストコンピュータ3側から変更可能である。また、万一CAT1が盗難にあい、窃盗犯が写真データから正規ユーザの顔についての特徴点を抽出しようと試みても、顔面特徴点データは得られないようになっている。さらに暗号化回路のキーは不定期に変更できるようにしてあり、仮に解読したとしても暗号化のアルゴリズム等が変わるようになっている。このため、同じキーを店舗に設置してあるCAT1からデータ送信することはできない。

【0043】また、制御部24に送られた各種データに基づいて、表示部10には必要情報が表示される。

【0044】CAT1から送信されたデータは、通信部17を経由して暗号解読部18に送られる(矢印104, 126参照)。そして、暗号解読部18によって解読されたデータは、CPU部25に送信され、そこで必要な演算処理を実行してから通信部17、閾値設定部23、判定指示部20に送られる(矢印128, 130, 134, 136参照)。また、CPU部25とデータベースファイル部19との間では、相互にデータのやり取りが行われる(矢印132, 138参照)。

【0045】判定指示部20による判定結果は、通信部17に送られ(矢印140参照)、その後CAT1の通信回路13に公衆回線や専用回線を通じて送られる(矢印140, 104参照)。

【0046】前記判定結果とは、例えば、カードユーザのブラックリストチェックやカードの有効期限チェックなどを行った結果ホストコンピュータ3でカード利用が

正当か否かの判定内容や正規ユーザの写真データの表出を例示できる。

【0047】通信回路13を経由してCAT1に入った判定結果は、制御部24を経由して表示部10に表示される。表示部10に表示された内容によりオペレータは正規ユーザによる有効なカード利用であるか否かがわかる。

【0048】そして、正規ユーザによる有効なカード利用であることが判明し、カード2の有効性について確認が取れた場合、CAT1はその制御部24によりプリンタ制御部21を経由してプリンタ部22を作動させ、伝票を印刷する(矢印118, 120参照)。

【0049】次に図6および図7のフローチャートを参照して本システムの流れを説明する。

【0050】本システムは、以下に述べるステップ101〜ステップ120からなる。なおステップを例えばS101と記号Sを用いて表記する。

【0051】S101では、カード2を利用して買物等を行いたいと思う顧客が加盟店の店員にその旨を告げると、店員はカード利用者である顧客からカード2を受け取り、CAT1によるクレジット売上げ承認の開始をオペレータとして実行する。

【0052】S102では、オペレータである店員が、カード2に表示されている写真とカード利用者とが同一人であるかをまず目視確認する。そして、同一人と判断(肯定判定)すればS103に進み、別人と判断(否定判定)すればS104に進む。フローチャートでは、等記号を用いた“カード写真=本人顔?”という表記で判定を実行することを示す。

【0053】S103では、店員は商品の値段である売上金額やその支払回数をどうするかについて顧客に問い合わせ、その内容をテンキー入力部11やファンクションキー部12の操作によって入力する。

【0054】S105ではカードリーダ部9でクレジットカード2の読み取りを行い、カード2が有する前記各種情報がCAT1に取り込まれる。

【0055】S106ではカード2の内部メモリに記憶した正規ユーザの顔面特徴点データが読み取られ、CAT1の表示部10に正規ユーザの顔面が表示される。

【0056】S109ではホストコンピュータ3の通信部17を経由してホストコンピュータ3に顔面特徴点データを送信する。

【0057】S110では、ホストコンピュータ3で判定を行う。

【0058】S111では、ホストコンピュータ3の通信部17を経由してホストコンピュータ3の判定結果をCAT1に送信する。

【0059】S112では、ホストコンピュータ3の通信部17を経由してホストコンピュータ3の判定結果をCAT1の表示部10に表示する。判定結果は前記閾値

による一致程度が幾らであるかで決定する。一致程度が0〜60%の場合は無条件にカードの利用を拒絶する。すなわち判定はNGとなる。一致程度が0〜60%以外の場合は、正規ユーザによる利用がなされていると判断されたか、またはどちらか不明であるという判断がされたことになる。

【0060】S112で否定判定した場合はS113に進み、肯定判定した場合は、S104に進む。

【0061】S113では一致程度が0〜60%の場合でないことを前提に一致程度が61〜80%か否かを判定する。S113で否定判定した場合はS115に進み、肯定判定した場合は、S116に進む。S113では、この内容を“判定グレー?”と表記する。

【0062】S115では一致程度が0〜80%でない場合、すなわち一致程度が81〜100%の場合であるから正規ユーザによるカードの利用と判定され取引が成立する。

【0063】S117ではプリンタ制御部21の制御によりプリンタ部22を作動してクレジット伝票の発行をする。

【0064】S118では顧客であるカード利用者に伝票へのサインを依頼し、S120で本システムによる取引を終了する。なお、取引がなされたことの証拠として、カード利用者にはカード裏面に記入されているサインと同じ形態のサインを伝票に記入してもらい、これをもって取引が成立する。当該取引データは、CAT内部にタンキングされる。そして、閉店時や営業時間中の指定時間中にホストコンピュータ3に取引トランザクションデータとして送信される。

【0065】S113で肯定判定した場合に進むS116ではカード利用者が正規ユーザか否か不明であるので、コンピュータによる判定ではなく人による再度の判定を行う。この内容を“取引有人再確認”と表記する。この判定を行うのにS119でクレジットカード会社の例えば電話センタに連絡する。

【0066】S119の次はS114に進む。S114では、S113と同様“判定がグレーか否か”を判定し、否定判定した場合はS115に進み、肯定判定した場合はS104に進む。

【0067】なお、CAT自体にまたはその近傍の店内適所に例えば電子スチルカメラを装備しておき利用者を撮影する。そして、CAT1から生の顔写真データをホストコンピュータ3に送信し、ホストコンピュータ3で顔の特徴点を抽出し、ホストコンピュータ3に格納してある顔面特徴点データと突き合わせるようにしてもよい。

【0068】次にこのような構成の本システムを利用したクレジットカードの不正使用防止技術の作用効果を述べる。

【0069】〈第一の不正防止効果〉本システムにあって

は、カード2内に従来のクレジット利用に不可欠なID等のデータに加え正規ユーザの顔面の写真データが記憶される。そして、ホストコンピュータ3ではその写真データから、カード表面上からは一切判明しない正規ユーザ判定用の顔面特徴点データを別途抽出する。また顔面特徴点データはデジタル化されてホストコンピュータ3のデータベースファイル部19に前記IDその他の個人情報と合わせて記憶されている。

【0070】よって、正規の利用者がカード2を利用すると、CAT1上の表示部10にカード2の内部メモリから読み取った写真データに基づいた顔写真が表出し、オペレータが正規ユーザによるカード利用の有無を目視で確認できる。この結果、カードの不正防止効果が高まる。

【0071】〈第二の不正防止効果〉カード2の写真データがCAT1で読み取られ特徴点が抽出される。抽出されたデータはCAT1内部の暗号化回路15により暗号化された顔面特徴点データ(顔画像データ全体ではない)だけでなく前記ID等の個人データがホストコンピュータ3に送信され正規ユーザであるか否かの本人照合がなされる。

【0072】なお、ホストコンピュータ3との間での通信途中に万一特徴点データが盗まれたとしても特徴点だけで正規利用者の顔を復元することは不可能である。よってセキュリティの向上を期待できる。

【0073】そしてホストコンピュータ3に記憶されている正規ユーザの顔画像データおよびホストコンピュータ3に送信されてきた各種データが一致すると、ホストコンピュータ3は利用者が正規ユーザであると判定してカード2の利用が可能であるという内容のメッセージ等をCAT1の表示部10に表示する。

【0074】ホストコンピュータ3に保管されているデータは、部外者が触れることのできない唯一の本人照合キーであることによる不正防止効果を図れる。

【0075】〈第三の不正防止効果〉カード2が盗難にあつてカード2の顔写真がすり替えられたとしても、CAT1の表示部10には、カード2の内部メモリに記憶されている写真データに基づいた正規ユーザの顔が表示される。この場合、カード2の顔写真とカード2の内部メモリに記憶されている写真データに基づいて表出される顔とは不一致である。よって、カード2の内部メモリに記憶されているデータが改竄されない限り、CAT1のオペレータは正規ユーザによるカード利用か否かを簡単に見分けられる。したがって不正使用は極めて難しくなる。

【0076】〈第四の不正防止効果〉高等技術の駆使により、盗んだカード2の顔写真をすり替えたり、またはカード2の内部メモリに記憶してある写真データをも入れ替えたりしても、ホストコンピュータ3に記憶されている正規ユーザの写真データと異なるため、カードの不正

使用を簡単に発覚できる。

【0077】〈第五の不正防止効果〉カードでなくCAT1が盗難されて盗難カードが擦られ、その内部メモリに不正使用をしようとする者の写真データがたとえ記憶されたとしても、ホストコンピュータ3に記憶されている正規ユーザの写真データが改竄されない限り、不正使用はできない。

【0078】〈第六の不正防止効果〉さらにセキュリティを高められるようにするために、カード2上の顔面データ読取時に暗号化回路15を通して抽出した顔面特徴点データにスクランブルをかけることも考えられる。

【0079】この場合、不定期に暗号化のアルゴリズムが変更されるので暗号化された特徴点はもとのオリジナルの特徴点を特定できない。よって、カードの不正使用を有効に防止できる。

【0080】(変形例) 顔面写真で照合する代わりに指紋で照合するようにしてもよい。

【0081】この場合、写真データの代わりに正規ユーザの指紋をデータ(以下「指紋データ」)として取り扱うようにし指紋データを解読し、ホストコンピュータに記憶してあった正規ユーザの指紋データと突き合わせるようにする。よってシステム上、カード2の内部メモリに指紋データを記憶する点、CAT1の顔面特徴点抽出部14が図示しない指紋特徴点抽出部になる点、ホストコンピュータ3のデータベースファイル部19に正規ユーザの指紋データが記憶される点が、写真データを用いる場合と相違する。

【0082】また、図8および図9は指紋照合を行う場合のフローチャートを示す。

【0083】このフローチャートが図6および図7のフローチャートと相違する点は、図6および図7のフローチャートに係るS106、S107、S108およびS112がそれぞれ、S206、S207、S208およびS212に変更された点と、S106およびS107にそれぞれ対応するS206およびS207の処理順序が前後する点である。よって、図6および図7のフローチャートと同一部分には同一符号を付して説明を省略する。

【0084】図8において、S105の次に進むS207では、カード2の内部メモリに記憶してある指紋データが正規ユーザの指紋か否かを判定する。肯定判定した場合は、S206に進み、否定判定した場合はS104に進む。

【0085】前記判定は等記号を用いて「カード内指紋データ=本人指紋?」と表記する。

【0086】S207で肯定判定した場合に進むS206では、カード2の内部メモリに記憶した正規ユーザの指紋データが読み取られ、CAT1の表示部10に正規ユーザの指紋照合が適正である旨を表示する。

【0087】S208では、当該カード2に記憶されて



ある指紋データを前記指紋特徴点抽出部により抽出し、その後暗号化回路によって抽出した指紋特徴データを暗号化する。

【0088】S212では、ホストコンピュータ3の通信部17を経由してホストコンピュータ3の判定結果をCAT1の表示部10に表示する。判定結果を閾値による一致程度が幾らであるかで決定するのは顔面特徴点データの場合と同じである。一致程度が0~60%の場合は無条件にカードの利用を拒絶する。すなわち判定はNGとなる。一致程度が0~60%以外の場合は、正規ユーザによる利用がなされていると判断されたか、またはどちらか不明であるという判断がされたことになる。

【0089】S212で否定判定した場合はS113に進み、肯定判定した場合は、S104に進む。

【0090】なお、顔面特徴点データや指紋データの代わりに周知のアイリス照合でも適用することが考えられる。

【0091】(応用例) 顔面特徴点データ、指紋データ等の適用技術の応用例として次のような場合が考えられる。

【0092】顔写真を内部メモリに記憶した身分証明カードを警備員に発行する。そして、警備員が規定の業務を遂行しているか否かがわかるよう、巡回先の適所に数箇所カード処理端末を設置する。そして、前記適所に警備員が巡回してきたらカードを読み込ませることで規定の業務を警備員が遂行しているか否かの判定をする。

【0093】また、銀行の貸金庫への出入口記憶レコーダとしての利用も考えられる。

【0094】さらに、例えばヘルスセンタ等における複数の商品売場での掛け売り処理を本人の顔画像データ等をキーとして行うことで、POS会計事務処理への適用ができる。

【0095】さらにまた、ホテル内でのレストラン等での部屋へつけ売りする場合の本人特定用に顔面照合等を適用することも考えられる。

【0096】加えて、プールでの料金精算にも利用できる。この場合も顔画像データ等をキーとして掛け売り金額をすべてPOSに記憶する。

【0097】さらに、レンタルビデオ店やレンタカー事務所での本人照合POSとして幅広い利用も考えられる。

【0098】また、車両の盗難防止を図るため、駐車場での運転者特定用のタイムレコーダとしても使える。

【0099】

【発明の効果】以上、説明したように本発明によれば、クレジットカードの不正使用を従来の技術よりも効果的に防止できる。

【図面の簡単な説明】

【図1】本発明に係るクレジットカードを利用した商品購入のシステムを示す概念図である。

【図2】本発明に係るクレジットカードの表面に記載の情報内容を示す図である。

10 【図3】本発明に係るクレジットカードの内部メモリに記憶されている情報内容を示す図である。

【図4】クレジットカードを利用した商品購入のシステムを示す概念図である。

【図5】図4に連続した図である。

【図6】本発明に係るクレジットカードを利用した商品購入のシステムを説明するためのフローチャートである。

【図7】図6に連続した図である。

20 【図8】本発明に係るクレジットカードを利用した商品購入のシステムの変形例を説明するためのフローチャートである。

【図9】図8に連続した図である。

【符号の説明】

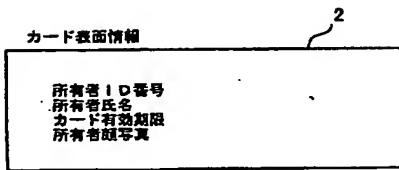
- 1 CAT (取引処理装置)
- 2 クレジットカード
- 3 ホストコンピュータ (センタ装置)
- 9 カードリーダ部 (読取手段)
- 10 表示部 (表示手段)
- 11 テンキー部
- 30 12 ファンクションキー部
- 13 通信回路 (送信手段)
- 14 顔面特徴点抽出部 (顔面特徴点抽出部)
- 15 暗号化回路
- 16 電源回路
- 17 通信部
- 18 暗号解読部
- 19 データベースファイル部
- 20 判定指示部
- 21 プリンタ制御部
- 40 22 プリンタ部
- 23 閾値設定部
- 24 制御部
- 25 CPU部



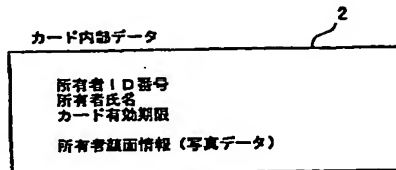
【図1】



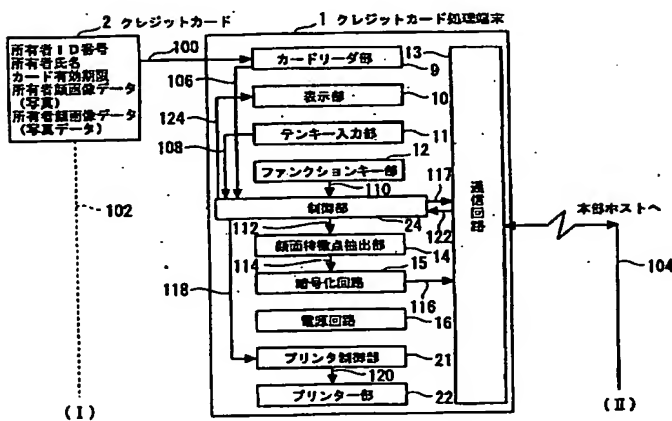
【図2】



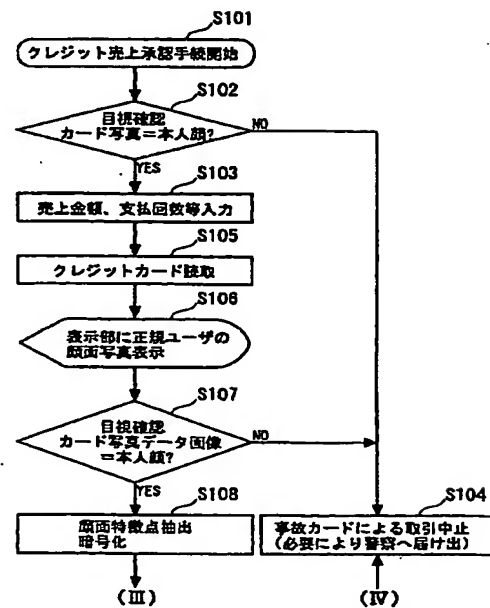
【図3】



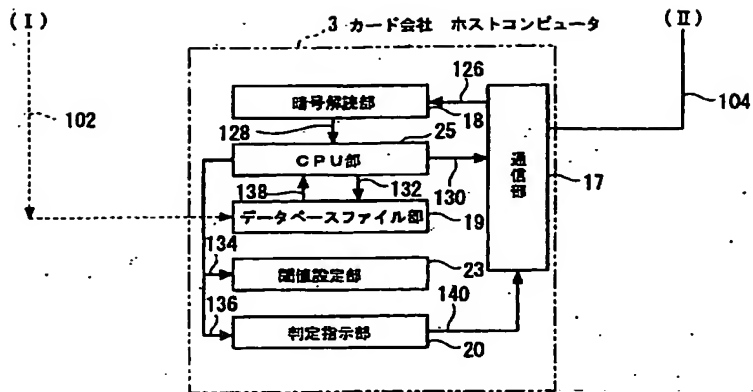
【図4】



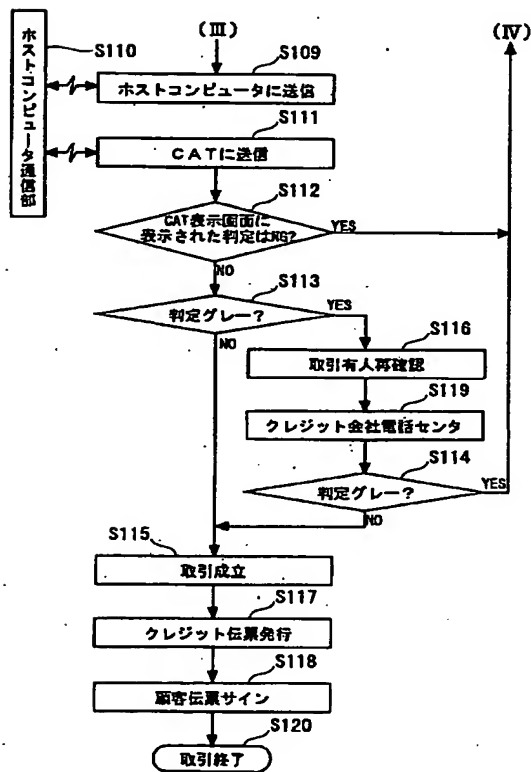
【図6】



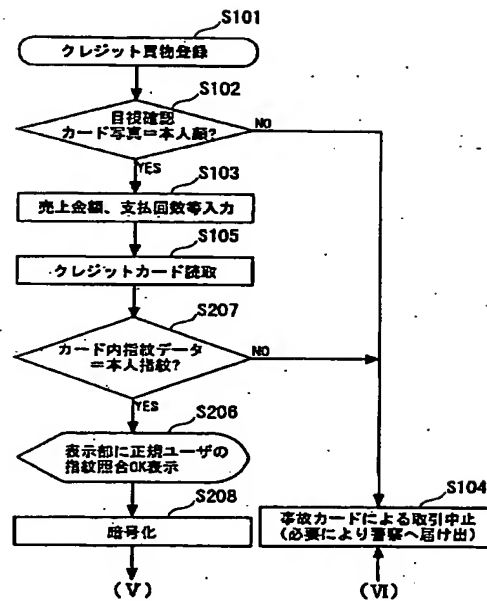
【図5】



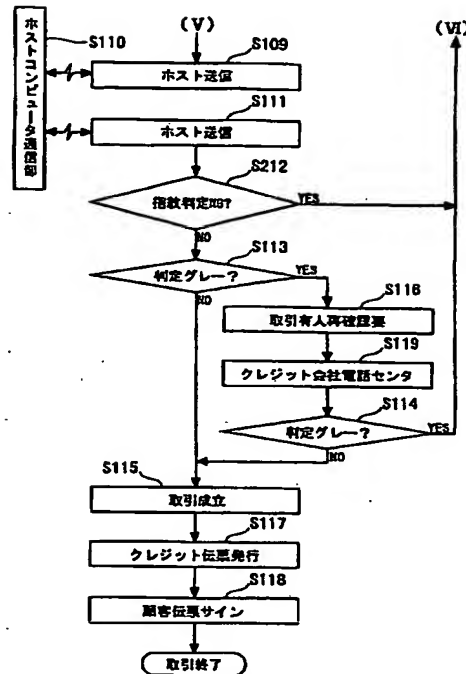
【図7】



【図8】



【図9】



フロントページの続き

(51) Int. Cl. 7	識別記号	F I	テマコード (参考)
G 0 6 K 17/00		G 0 6 K 17/00	L 5 J 1 0 4
			T 5 L 0 9 6
			V
19/00		G 0 6 T 1/00	3 4 0 A
19/10			3 0 0 F
G 0 6 T 1/00	3 4 0	H 0 4 L 9/00	6 7 3 D
7/00	3 0 0	G 0 6 K 19/00	Q
G 0 7 F 7/12			S
H 0 4 L 9/32		G 0 7 F 7/08	B

F ターム(参考) 2C005 HA03 HB01 HB07 HB09 HB20  
JA08 JB02 JB05 JB06 JB33  
LA29 LB32 LB34 MA04 MB01  
MB07 MB08 MB10 QC12 SA02  
SA14 SA15 SA16  
3E044 AA20 BA05 CA03 CA06 CA10  
DA05 DA10 DD01 DE01 DE02  
5B035 AA13 AA14 BB09 BB11 BC01  
CA06 CA29  
5B057 AA19 BA02 CA12 CA16 DA11  
DB02 DC01 DC36  
5B058 CA22 CA25 KA02 KA04 KA05  
KA06 KA08 KA31 KA35 KA37  
YA02  
5J104 AA07 EA22 KA16 MA01 NA33  
5L096 BA03 BA18 CA02 FA00 JA11